John R. Parker, Jr. (SBN 257761)
jrparker@almeidalawgroup.com
ALMEIDA LAW GROUP LLC
3550 Watt Avenue, Suite 140
Sacramento, California 95608
Tel: (916) 616-2936

David S. Almeida (*pro hac vice forthcoming*)
Matthew J. Langley, California Bar No. 342846
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
t: 312-576-3024
david@almeidalawgroup.com
matt@almeidalawgroup.com

Attorneys for Plaintiff and the Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

R.S., *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

PRIME HEALTHCARE SERVICES, INC.,

Defendant.

Case No. 5:24-cv-00330

CLASS ACTION COMPLAINT

FOR:

1. **ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2511(1), et seq.**

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff R.S. ("Plaintiff") brings this class action lawsuit individually and on behalf of all others similarly situated (the "Class Members") against Prime Healthcare Services, Inc. ("Prime Healthcare" or "Defendant"). The allegations set forth herein are based on Plaintiff's personal knowledge and on information and belief as to all other matters based upon investigation by counsel.

INTRODUCTION

1. Defendant Prime Healthcare is a privately held healthcare company established in 2001. Prime Healthcare is the fifth largest for-profit health system in the United States operating 44 hospitals in 14 states, including California. Prime Healthcare also operates more than 300 outpatient locations and has nearly 45,000 employees and affiliated physicians. [1]

2. As part of the medical services it provides, Prime Healthcare owns, controls and maintains websites for its hospitals ("Websites"), as well as web-based patient portals (the "Portals"). The Websites and the Portals are collectively referred to herein as the "Web Properties."

3. Among the hospital Websites and Portals owned and operated by Prime Healthcare are the following[2]:

- Chino Valley Medical Center - https://cvmc.com/

[1] *See* https://www.primehealthcare.com/ (last visited Jan. 22, 2024).

[2] In December 2023 UC San Diego Health completed the purchase of Alvarado Hospital Medical Center from Defendant. However, Prime Healthcare owned the hospital in question during the relevant time period. *See* https://thecoastnews.com/ucsd-completes-200-mil-purchase-of-alvarado-hospital/ (last visited Feb. 6, 2024).

- Centinela Hospital Medical Center - https://centinelamed.com/
- Desert Valley Hospital - https://dvmc.com/
- Encino Hospital Medical Center - https://encinomed.org/
- Paradise Valley Hospital - https://paradisevalleyhospital.net/
- Sherman Oaks Hospital - https://shermanoakshospital.org/
- Alvarado Hospital Medical Center - https://alvaradohospital.com/
- North Vista Hospital - https://northvistahospital.com/
- Garden City Hospital - https://gch.org/
- Monroe Hospital - https://monroehospital.com/
- St. Joseph Medical Center - https://stjosephkc.com/
- Lower Bucks Hospital - https://lowerbuckshosp.com/
- Suburban Community Hospital - https://suburbanhosp.org/
- St. Mary's General Hospital - https://smh-nj.com/
- St. Clare's Dover Hospital - https://saintclares.com/
- East Liverpool City Hospital - https://elch.org/

4. Prime Healthcare actively encourages its patients to use its Web Properties to communicate with their healthcare providers; access lab and test results; manage prescriptions and request refills; manage medical appointments; search medical conditions and treatment options; and much more. The Web Properties are set up to mimic the in-person visit and invite patients to share and search for personal medical information about their own physical and mental health. And patients, trusting that this information will be safeguarded, share intimate and personal medical information with Prime Healthcare through the Web Properties.

5. Information concerning a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of such information can have serious consequences, including, but certainly not limited to, discrimination in the workplace and/or denial of insurance coverage.[3]

Defendant Utilized Tracking Technologies to Monetize Users' Private Information.

6. Plaintiff and Class Members who visited and used Prime Healthcare's Web Properties (collectively, the "Users") reasonably believed that they were communicating only with their trusted healthcare providers.

7. At no point has Prime Healthcare, despite intentionally incorporating a tracking Pixel into its Websites and servers, informed Users that their personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "PII/PHI" or "Private Information") communicated via its Web Properties was intentionally disclosed to a third party—let alone Facebook[4], which has a sordid history of privacy violations.[5]

---

[3] *See* Lindsey Ellefson, *Telehealth Sites Put Addiction Patient Data at Risk: New research found pervasive use of tracking tech on substance-abuse-focused health care websites, potentially endangering users in a post-Roe world*, WIRED (Nov. 16, 2022), https://www.wired.com/story/substance-abuse-telehealth-privacy-tracking-tech/ (last visited Feb. 6, 2024) ("While the sharing of any kind of patient information is often strictly regulated or outright forbidden, it's even more verboten in addiction treatment, as patients' medical history can be inherently criminal and stigmatized.").

[4] Meta Platforms, Inc. is doing business as "Meta" and "Facebook." The terms "Meta" and "Facebook" are used interchangeably throughout.

[5] This Court will not have to look far to find evidence of Meta's violations of

8. However, unbeknownst to Plaintiff and Class Members, Defendant installed tracking technologies on its Web Properties to collect and disclose their Private Information to unauthorized third parties for its own pecuniary gain.

9. Specifically, Defendant embedded undetectable tracking Facebook pixels (the "Pixels" or "Facebook Pixels") on its Web Properties, including the Websites, which transmit an incredible amount of personal and protected data about its Users to Meta Platforms, Inc., d/b/a Meta ("Meta" or "Facebook"). The collection and transmission of this information is instantaneous, invisible and occurs without any notice to—and certainly no consent from—the Users.[6]

10. The Facebook Pixel, installed and configured by Defendant, is a piece of code that "tracks the people and [the] type of actions they take"[7] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature or text box).

---

privacy laws. Just in May of last year, for instance, the European Union fined Meta "a record-breaking" $1.3 billion for violating EU privacy laws. *See* Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html (last visited Feb. 6, 2024).

[6] Healthcare providers that use analytics tools like the Facebook Pixel or Google Analytics on their websites may also have those tools embedded on a patient portal login page or even inside a patient portal.

[7] *Retargeting*, https://www.facebook.com/business/goals/retargeting (last visited Jan. 31, 2023).

11. The pixels—which are configured by the website owners, here, Prime Healthcare—collect and transmit information from Users' browsers to unauthorized third parties, including, but not limited to, Facebook.[8]

12. Together with the patients' Private Information, the data sent to Facebook also discloses Users' unique and persistent Facebook ID ("Facebook ID" or "FID") which allows Facebook (and other third parties) to personally identify those Users and associates their Private Information with their Facebook profile.[9]

Defendant's Disclosure of Private Information Without Consent Violates the Law.

13. In recent months, and in stark contrast to Prime Healthcare, several medical providers that used the Facebook Pixel in a similar way have provided their patients with notices of data breaches caused by the Pixel transmitting their information to third parties.[10]

---

[8] The pixel itself is a small snippet of code placed on webpages by the website owner. The process of adding the pixel to a webpage is a multi-step process that, as described in detail in *section E*, must be undertaken by the website owner such as Defendant.

[9] The Facebook ID is a unique string of numbers Facebook uses to identify and connect to a User's Facebook profile via, among other methods, a *c_user* cookie. Facebook creates a Facebook ID automatically, whether or not you choose to create a username. Thus, Facebook, which creates and maintains the Facebook ID directly connected to a User's Facebook account, utilizes the Facebook ID to personally identify each User whose Private Information is disclosed to it. *See Facebook Cookies Analysis*, https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a; *see also* https://www.cyberseo.net/blog/how-to-get-facebook-c_user-and-xs/ (last visited Feb. 6, 2024).

[10] *See, e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, available at https://cerebral.com/static/hippa_privacy_breach-

14. Simply put (and as detailed herein), covered entities such as Prime Healthcare are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third party without express and informed consent from each patient. Neither Plaintiff nor any other Class Members were provided—much less signed—a written authorization permitting Prime Healthcare to disclose their Private Information to Facebook or any other third-party data brokers.

15. As recognized by both the Federal Trade Commission ("FTC") and the Office for Civil Rights ("OCR") of the Department of Health and Human Services ("HHS"), healthcare companies' use of tracking technologies to collect and divulge their patients' sensitive and confidential information is an extremely serious data security and privacy issue:

> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***[11]

4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Feb. 6, 2024); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies* (Oct. 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3 (last visited Feb. 6, 2024); *Novant Health Notifies 1.36 Million Patients About Unauthorized Disclosure of PHI via Meta Pixel Code on Patient Portal* (Aug. 16, 2022), https://www.hipaajournal.com/novant-health-notifies-patients-about-unauthorized-disclosure-of-phi-via-meta-pixel-code-on-patient-portal/ (last visited Feb. 6, 2024).

[11] *See* Elisa Jillison, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases,* the FTC Business Blog (July 25, 2023) (emphasis added), https://www.ftc.gov/business-

16. Similarly, OCR is clear that "[r]egulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."[12]

17. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This information can be used to identify, contact or locate a single person or can be used with other sources to identify a single individual.

18. These HIPAA Identifiers, as relevant here, include device identifiers, web URLs, and IP addresses.[13]

Defendant Derives Significant Value from Users' Private Information

19. There is no anonymity in the information disclosed to Facebook for marketing and analytics purposes; that is, the Pixel collects and discloses a substantial "data packet" coupled with the FID so that Prime Healthcare can, among other things, send targeted advertisements to Users based on

---

guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases (last visited Feb. 6, 2024).

[12] OCR Bulletin, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis added) (last visited Feb. 6, 2024).

[13] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 11, 2024).

their sensitive and protected Private Information. Prime Healthcare also uses this impermissibly obtained data for analytics purposes to gain additional insights into how its patients use its Web Properties. [14]

20. Operating as designed and as implemented by Prime Healthcare, the Pixel disclosed information that allows a third party (*e.g.*, Facebook) to know when and where a specific patient was seeking confidential medical care, the medical condition(s) that patient inquired about, and the precise care the patient sought or received. Facebook, in turn, sells Plaintiff's and Class Members' Private Information to third-party marketers who geo-target Plaintiff's and Class Members' Facebook accounts based on that Private Information.

21. While the information captured and disclosed without permission may vary depending on the pixel(s) embedded, these "data packets" can be extensive, sending, for example, the User's first name, last name, email address, phone number, zip code, and city of residence entered on the Web Properties. The data packets also include the buttons a User clicks and the exact words a User types into a search bar.

22. For instance, when a User uses Prime Healthcare's Web Properties where tracking technologies, such as the Facebook Pixel are present, the Pixel transmits the contents of their communications to Facebook, including, but not limited to: (i) accessing the patient portal; (ii)

---

[14] Prime Healthcare unquestionably is required to inform its Users if it deploys tracking technologies on its Web Properties so that Users can make informed decisions as to whether they want their information to be collected, disclosed, and used in this manner. The OCR Bulletin is, again, instructive: "disclosures of PHI to tracking technology vendors for marketing purposes, ***without individuals' HIPAA-compliant authorizations,*** would constitute impermissible disclosures." *See* OCR Bulletin, *supra* note 12.

the exact text of the User's search queries; (iii) medical services and treatments sought; (iv) scheduling of appointments; (v) accessing and viewing the bill page; (vi) the text of URLs visited by the User; and (vii) other information that qualifies as PII and PHI under federal and state laws. The data in the "data packets" is then linked to a specific internet protocol ("IP") address, which is itself protected information under the Health Insurance Portability and Accountability Act ("HIPAA").

23. By installing the Facebook Pixel and other tracking technologies, Prime Healthcare effectively planted a bug on Plaintiff's and Class Members' web browsers and caused them to unknowingly disclose their private, sensitive and confidential health-related communications to Facebook.[15]

24. The information intercepted by the Pixels and third-party tracking technologies is used to build incredibly fulsome and robust marketing profiles for individual Users and create targeted advertisements based on the medical conditions and other Private Information disclosed. Despite the clear and unequivocal prohibition on the disclosure of PHI without consent, Prime Healthcare chose to use the Pixel data for marketing purposes to bolster its revenue.

25. Simply put, Prime Healthcare puts its desire for revenue over its patients' privacy rights.

Defendant's Conduct Caused Concrete & Demonstrable Harm to Users.

[15] While this Amended Complaint primarily focuses on how Prime Healthcare embedded the Pixel on its Web Properties to collect and disclose Users' Private Information, other secret tracking technologies embedded by Prime Healthcare—such as, for example, Google Analytics—also collect such Private Information, and the respective tech companies have the capability to link it to specific user profiles.

26. As a healthcare provider, Prime Healthcare has certain duties and obligations to its patients. Prime Healthcare breached those duties and obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web-based technology to ensure the Web Properties were safe and secure; (ii) failing to remove or disengage technology that was known and designed to share Web Properties' Users' information; (iii) failing to obtain the consent of Plaintiff and Class Members to disclose their PII and PHI to Facebook or other third parties; (iv) failing to take steps to block the transmission of Plaintiff's and Class Members' PII and PHI through the Pixels; (v) failing to warn Plaintiff and Class Members about the tracking technology; and (vi) otherwise failing to design and monitor its Web Properties to maintain the confidentiality and integrity of patient PII and PHI.

27. Plaintiff and Class Members have suffered injury because of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) compromise and disclosure of Private Information; (iv) diminution of value of their Private Information; (iv) statutory damages; and (v) the continued and ongoing risk to their Private Information.[16]

28. Plaintiff seeks to remedy these harms for herself and a class of all others similarly situated.

PARTIES

[16] The exposed Private Information of Plaintiff and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or insurance companies utilizing the information to set insurance rates. Furthermore, third parties often offer the unencrypted, unredacted Private Information for sale to criminals on the dark web for use in fraud and cyber-crimes.

29. Plaintiff R.S. is a natural person and resident of the city of Inglewood in Los Angeles County, California.

30. As detailed herein, Plaintiff accessed Prime Healthcare's Web Properties on her computer and mobile devices and used the Web Properties to look for providers, review conditions and treatments, make appointments, and communicate with her healthcare providers. Plaintiff has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

31. Defendant Prime Healthcare is a Delaware corporation with its principal place of business and corporate headquarters at 3480 E. Guasti Road, Ontario, in San Bernadino County, California.

32. Defendant is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

JURISDICTION AND VENUE

33. This Court has "federal question" jurisdiction given the federal claims alleged by Plaintiff. This Court also has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

34. The Court has personal jurisdiction over Defendant because its principal place of business and headquarters are located in San Bernadino County in the city of Ontario, State of California, it regularly engages in business in the State of California and in County of San Bernadino, and a substantial portion of the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this county.

35. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because: a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the unauthorized sharing of Plaintiff's and Class Members' Private Information; Defendant's principal place of business is located in this District; Defendant collects and redistributes Class Members' Private Information in this District and Defendant caused harm to Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Federal Regulators Make Clear that the Use of Tracking Technologies to Collect & Divulge Private Information Without Informed Consent is Illegal.

36. Prime Healthcare's surreptitious collection and divulgence of Private Information is an extremely serious data security and privacy issue. Both the Federal Trade Commission ("FTC") and the Office for Civil Rights of the HHS have—in recent months—reiterated the importance of and necessity for data security and privacy concerning health information.

37. For instance, the FTC recently published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. ***Rather, it is anything that conveys information—or enables an inference—about a consumer's health***. Indeed, [recent FTC enforcement actions involving] *Prenom, BetterHelp, GoodRx, and Flo Health* ***make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or***

fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."[17]

38. The FTC is unequivocal in its stance as it informs—in no uncertain terms—healthcare companies that they should ***not*** use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.**
>
> In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. ***But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out.***
>
> [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that ***may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information***.[18]

39. The federal government is taking these violations of health data privacy and security seriously, evidenced by recent high-profile FTC settlements against several telehealth companies.

---

[17] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases, supra*, note 11 (emphasis added) (visited Feb. 6).

[18] *Id.* (emphasis added) (further noting that *GoodRx* & *Premom* underscore that this conduct may also violate the Health Breach Notification Rule, which requires notification to consumers, the FTC and, in some cases, the media, of disclosures of health information without consumers' authorization).

40. For example, the FTC recently imposed a $1.5 million penalty on GoodRx for violating the FTC Act by sharing its customers' sensitive PHI with advertising companies and platforms, including Facebook, Google and Criteo. The FTC also reached a $7.8 million settlement with the online counseling service BetterHelp, resolving allegations that the company shared customer health data with Facebook and Snapchat for advertising purposes. Likewise, the FTC reached a settlement with Flo Health, Inc. related to information about fertility and pregnancy that Flo fertility-tracking app was improperly sharing with Facebook, Google, and other third parties. And Easy Healthcare was ordered to pay a $100,000 civil penalty for violating the Health Breach Notification Rule when its ovulation tracking app, Premon, shared health data for advertising purposes.[19]

41. Even more recently, in July 2023, federal regulators sent a letter to approximately 130 healthcare providers warning them about using online

[19] *See* How FTC Enforcement Actions Will Impact Telehealth Data Privacy, https://healthitsecurity.com/features/how-ftc-enforcement-actions-will-impact-telehealth-data-privacy (last visited Feb. 6, 2024); *see also* Allison Grande, *FTC Targets GoodRx In 1st Action Under Health Breach Rule*, Law360 (Feb. 1, 2023), available at www.law360.com/articles/1571369/ftc-targets-goodrx-in1st-action-under-health-breach-rule?copied=1 ("The Federal Trade Commission signaled it won't hesitate to wield its full range of enforcement powers when it dinged GoodRx for allegedly sharing sensitive health data with advertisers, teeing up a big year for the agency and boosting efforts to regulate data privacy on a larger scale."); https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-gives-final-approval-order-banning-betterhelp-sharing-sensitive-health-data-advertising; https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc; https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google (last visited Feb. 6, 2024).

tracking technologies that could result in unauthorized disclosures of Private Information to third parties. The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others." According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[20]

42. The OCR has made clear, in a recent bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[21]

43. The OCR Bulletin *reminds* healthcare organizations regulated under HIPAA that they may use third-party tracking tools, such as Google Analytics or Pixels *only in a limited way* to perform analysis on data key to

[20] *See* OCR Bulletin, *supra* note 12.

[21] *Id*.

operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[22]

44. The OCR Bulletin discusses the harms that disclosure may cause patients:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI.*** Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment.*** While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[23]

45. Moreover, investigative journalists have published several reports detailing the seemingly ubiquitous use of tracking technologies on the digital properties of hospitals, health care providers and telehealth companies to monetize their Users' Private Information.

46. For instance, THE MARKUP reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a

[22] *See id*.

[23] *Id.* (emphasis added).

packet of data whenever a person clicked a button to schedule a doctor's appointment.[24]

47. And, in the aptly titled report *"Out of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, a joint investigation by STAT and THE MARKUP of 50 direct-to-consumer telehealth companies reported that telehealth companies or virtual care websites were providing sensitive medical information they collect to the world's largest advertising platforms.[25]

48. Many healthcare sites had at least one tracker—from Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn, and/or Pinterest—that collected patients' answers to medical intake questions.[26]

B. Tracking Pixels.

49. Pixels are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting, for example, serving

---

[24] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Feb. 6, 2024).

[25] Todd Feathers, Katie Palmer (STAT) & Simon Fondrie-Teitler, *"Out Of Control": Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies: An investigation by The Markup and STAT found 49 out of 50 telehealth websites sharing health data via Big Tech's tracking tools* (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies (last visited Feb. 6, 2024).

[26] *See id.* (noting that "[t]rackers on 25 sites, including those run by industry leaders Hims & Hers, Ro, and Thirty Madison, told at least one big tech platform that the user had added an item like a prescription medication to their cart, or checked out with a subscription for a treatment plan").

online advertisements to people who have previously engaged with a business's website—and other marketing.

50. Here, a User's web browser executes the Pixels via instructions within each webpage of Prime Healthcare's Websites (and, upon information and good faith belief, within Prime Healthcare's Patient Portals) to communicate certain information (within parameters set by Prime Healthcare) directly to Facebook—at the same time as the User's browser is sending this information to Prime Healthcare.

51. The Pixels can also share the Users' identifying information for easy tracking via "cookies"[27] stored on their computer by Facebook. For example, Facebook stores or updates a Facebook-specific cookie every time a person accesses their Facebook account from the same web browser.

52. The Facebook Pixel can access this cookie and send certain identifying information like the User's Facebook ID to Facebook along with the other data relating to the User's Website inputs. The same is true for other tracking code information recipients, which also create cookies that are stored in the User's computer and accessed by their tracking codes to identify the User.

53. The Pixels are programmable, meaning that Prime Healthcare controls which of the webpages on the Website contain the Pixels and which events are tracked and transmitted to Facebook (or other unauthorized third party data brokers whose tracking codes are embedded by Defendant on its Web Properties).

---

[27] "Cookies are small files of information that a web server generates and sends to a web browser Cookies help inform websites about the user, enabling the websites to personalize the user experience." *See* https://www.cloudflare.com/learning/privacy/what-are- cookies/ (last visited Feb. 6, 2024).

54. Prime Healthcare has utilized Facebook Pixels (and, upon information and good faith belief, other tracking technologies such as Google Analytics) since at least October 2018.

55. Prime Healthcare used the data it collected from Plaintiff and Class Members, without their consent, to improve its advertising and bolster its revenue.

C. Conversions API.

56. In addition to the Facebook Pixel, Facebook Conversions API and similar tracking technologies allow businesses to send web events, such as clicks, form submissions, keystroke events and other actions performed by the user on the Website, from their own servers to Facebook and other third parties.[28]

57. Conversions API creates a direct and reliable connection between marketing data (such as website events and offline conversations) from Prime Healthcare's server to Facebook.[29] In doing so, Prime Healthcare stores Plaintiff's and Class Members' Private Information on its own server and then transmits it to unauthorized third parties like Facebook.

58. Conversions API is an alternative method of tracking versus the Meta Pixel because no privacy protections on the user's end can defeat it. This is because it is "server-side" implementation of tracking technology, whereas pixels are "client-side"—executed on users' computers in their web browsers.

---

[28] *See* https://revealbot.com/blog/facebook-conversions-api/ (last visited Feb. 6, 2024).

[29] *See* https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Feb. 6, 2024).

59. Because Conversions API is server-side, it cannot access the Facebook *c_user* cookie to retrieve the Facebook ID.[30] Therefore, other roundabout methods of linking the user to their Facebook account are employed.[31] For example, Facebook has an entire page within its developers' website about how to de-duplicate data received when both the Facebook Pixel and Conversions API are executed.[32]

60. Conversions API tracks the user's website interactions, including Private Information being shared, and then transmits this data to Facebook and other third parties. Facebook markets Conversions API as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[33]

---

[30] "Our systems are designed to not accept customer information that is unhashed Contact Information, unless noted below. Contact Information is information that personally identifies individuals, such as names, email addresses and phone numbers, that we use for matching purposes only." *See* https://developers.facebook.com/docs/marketing-api/conversions-api/parameters/customer-information-parameters/ (last visited Feb. 6, 2024).

[31] "Sending additional customer information parameters may help increase Event Match Quality. Only matched events can be used for ads attribution and ad delivery optimization, and the higher the matching quality, the better." https://developers.facebook.com/docs/marketing-api/conversions-api/best-practices/#req- rec-params (last visited Feb. 6, 2024).

[32] *See* https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel- and-server-events (last visited Feb. 6, 2024).

[33] *About Conversions API*, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Feb. 6, 2024).

61. Prime Healthcare installed the Meta Pixel and, upon information and good faith belief, Conversions API, as well as other tracking technologies, on many (if not all) of the webpages within its Web Properties (including the member-only patient portal) and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Pixel Information Recipients—communications that included Plaintiff's and Class Members' Private Information.

D. Prime Healthcare's Method of Transmitting Plaintiff's & Class Members' Private Information via Pixels.

62. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (computer, tablet or smartphone) accesses web content through a web browser (*e.g.*, Google's Chrome, Mozilla's Firefox, Apple's Safari, and/or Microsoft's Edge browsers).

63. Every website is hosted by a computer "server" that holds the website's contents. The entity(ies) in charge of the website exchange communications with users' devices as their web browsers query the server through the internet.

64. Web communications consist of Hypertext Transfer Protocol ("HTTP") or Hypertext Transfer Protocol Secure ("HTTPS") requests and HTTP or HTTPS responses, and any given browsing session may consist of thousands of individual HTTP requests and HTTP responses, along with corresponding cookies:

1. **HTTP request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can

also send data to the host server embedded inside the URL and can include cookies. POST Requests can send a large amount of data outside of the URL. (For instance, uploading a PDF to file a motion to a court.)

2. **Cookies**: a small text file that can be used to store information on the client device that can later be communicated to a server or servers. Cookies are sent with HTTP requests from client devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website.

3. **HTTP response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP request. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data.

65. A patient's HTTP request essentially asks Prime Healthcare's Website to retrieve certain information (such as a set of health screening questions). The HTTP response sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons and other features that appear on the participants' screens as they navigate Prime Healthcare's Website.

66. Every website is comprised of Markup and "Source Code." Source Code is a simple set of instructions that commands the website user's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

67. Source Code may also command a web browser to send data transmissions to third parties in the form of HTTP requests quietly executed in the background without notifying the web browser's user.

68. The Pixels are Source Code that do just that—they surreptitiously transmit a Website User's communications and inputs to the corresponding Pixel Information Recipient, much like a traditional wiretap. When individuals visit Prime Healthcare's Website via an HTTP request to

Prime Healthcare's server, Prime Healthcare's server sends an HTTP response (including the Markup) that displays the webpage visible to the User, along with Source Code (including the Pixels).

69. Thus, Prime Healthcare is, in essence, handing its patients a tapped website and, once a webpage is loaded into the patient's browser, the software-based wiretaps are quietly waiting for private communications on the webpage to trigger the Pixels, which then intercept those communications—intended only for Prime Healthcare—and instantaneously transmit those communications to Facebook (or, in case of other invisible tracking codes, to another corresponding recipient of information captured bysuch technology).

70. Third parties like Facebook place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third party can identify the specific user associated with the information intercepted (in this case, highly sensitive Private Information).

71. Prime Healthcare intentionally configured Pixels installed on its Web Properties to capture both the "characteristics" of individual patients' communications with Prime Healthcare's Websites (their IP addresses, Facebook ID, cookie identifiers, device identifiers, and account numbers) and the "content" of these communications (the buttons, links, pages, and tabs they click and view related to their health conditions and services sought from Defendant).

72. Prime Healthcare's patient portal software system was also designed to permit licensees—such as Prime Healthcare—to deploy "custom analytics scripts" within the Portal. For example, this would allow the website owner to deploy the Facebook Pixel or Google Analytics to capture

the transmission of Private Information, including medical and health-related information and communications to third parties.[34]

73. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Facebook:

a. Plaintiff's and Class Members' status as medical patients;

b. Plaintiff's and Class Members' communications with Defendant through its Web Properties, including specific text queries typed into the search bar, medical conditions for which they sought treatments and treatments sought;

c. Plaintiff's and Class Members' searches for appointments, appointment details, location of treatments, medical providers' names and their specialties, medical conditions, and treatments; and

d. PII, including but not limited to patients' locations, IP addresses, device identifiers and an individual's unique Facebook ID.

74. Through the Prime Healthcare Web Properties, Defendant shares its patients' identities and online activity, including information and search results related to their private medical treatment.

75. When they visit the Websites, Prime Healthcare patients can search for a doctor by selecting the "Find a Doctor" button. Patients are then directed to the "Find a Doctor" pop-up shown below where they can search for a doctor by specialty and location or by simply entering a particular doctor's name.

76. When a patient searches for a doctor, the search information is

[34] *See* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Feb. 6, 2024).

sent directly to Facebook. For example, when a patient searches for a female cancer (oncology/hematology) specialist in a specified location, that information is sent to Facebook, along with which doctors are shown in search results.

77. When patients select a doctor, this information is automatically sent directly to Facebook. For example, when a patient clicks on a particular physician's name, they are directed to that physician's profile. At that time, the information is automatically sent directly to Facebook, alongside the particular patient's Facebook ID ("FID").

78. Here, the search parameters set by the patient and the patient's FID number are being shared together, thereby allowing Facebook to make the direct connection between the search parameters and each individual patient's FID. Even without the FID, other identifying information like IP address or device identifier is captured by the Pixel and transmitted to Facebook.

79. Facebook categorizes this event as a "PageView," which indicates that the patient viewed the webpage.

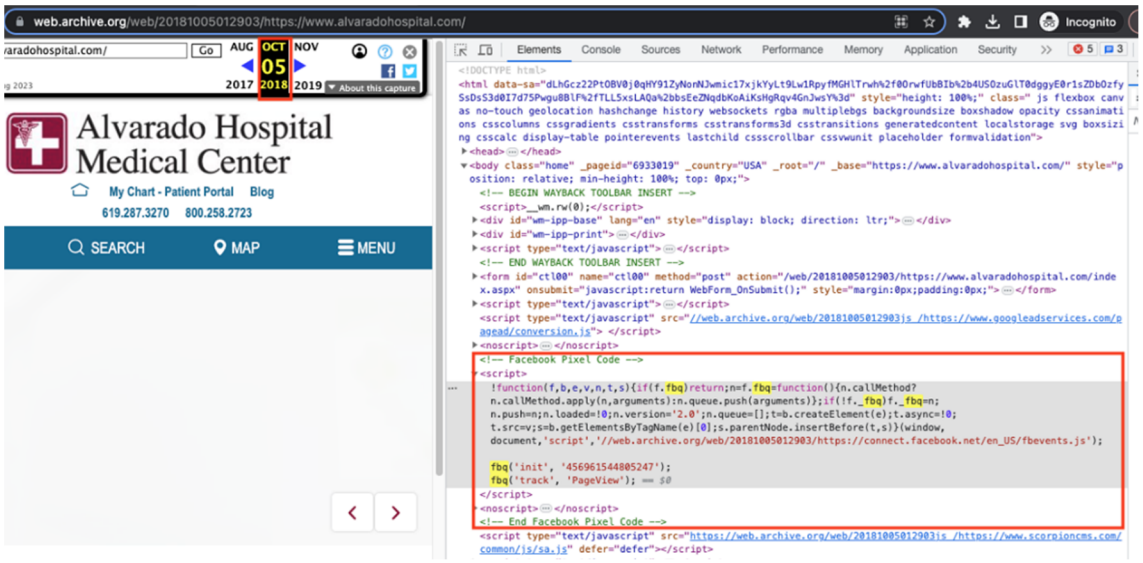
80. The information Defendant shares with Facebook during a patient's use of the appointment booking tool and "find a doctor" tool enables Facebook to identify what type of doctor each patient is searching for, and Defendant is sharing this information without its patients' knowledge or consent.

81. Every time Defendant sends a patient's Website activity data to Facebook, that patient's personally identifiable information is also disclosed, including their FID. An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any

individual on its Facebook platform with only their unique FID, so too can any ordinary person who knows or has acquired someone's FID. Facebook admits as much on its website. Indeed, ordinary persons who come to acquire an FID can connect to the corresponding Facebook profile.

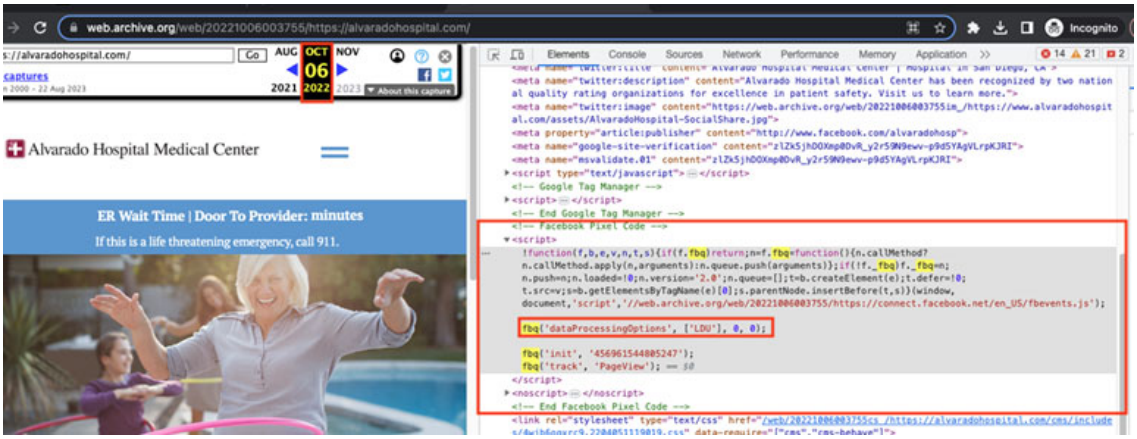
82. A user who accesses Defendant's Websites while logged into Facebook will transmit the c_user cookie to Facebook, which contains that user's unencrypted Facebook ID. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies embedded on Prime Healthcare's website to link to FIDs and corresponding Facebook profiles.

83. Prime Healthcare installed the Meta Pixel ID 456961544805247 ("Prime Pixel"), directly in the website's HTML source code from as early as October 5, 2018 and as recently as October 6, 2022. *See* Figure 1:



84. Prime Healthcare currently has data protection mode enabled for Facebook Events, however as demonstrated by screenshots captured on October 6, 2022, Prime Pixel previously did not have data protection mode

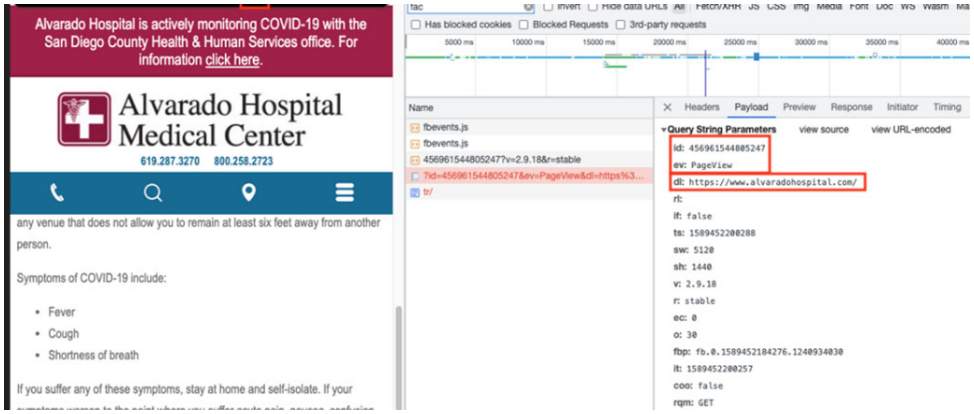
enabled.[35] *See* Figure 2:

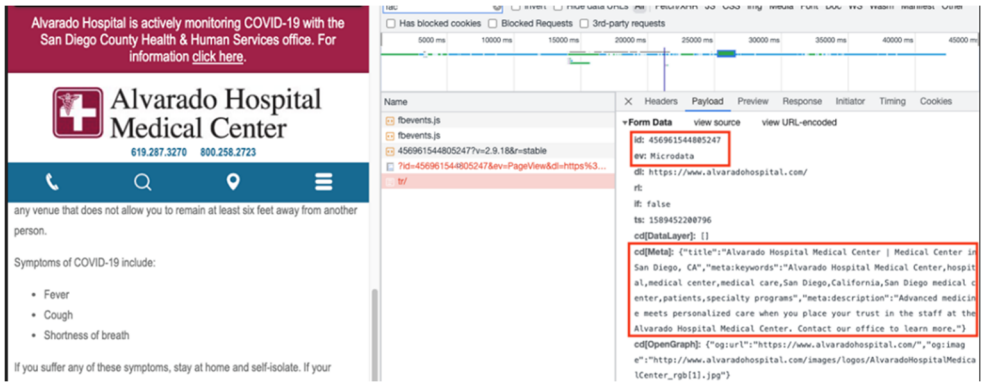


85. By modifying Prime Pixel's configuration to disable data protection mode, one can observe the sort of Meta Pixel events that Prime Healthcare would have previously sent (tied to each User's unique Facebook ID) at the time the Plaintiff used Prime Healthcare's Web Properties.

86. For example, upon a User's arrival on Prime Healthcare's homepage for Alvarado Hospital, Prime Healthcare sent this information to Facebook via both PageView and Microdata events, disclosing that the user was on the page, https://alvaradohospital.org/. *See* Figures 3-4:

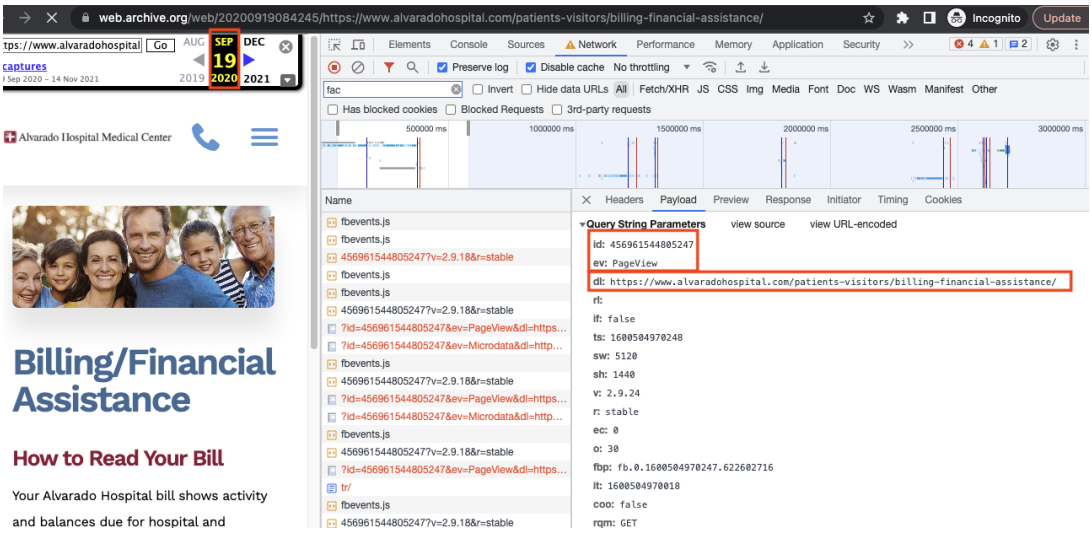
[35] Meta provides a tool called "data processing options," to comply with state privacy laws. The tool limits Meta's use of the data the Meta Pixel sends. *See* https://developers.facebook.com/docs/marketing-apis/data-processing-options/. The tool can be configured to apply a particular state's policy to all users or it can use geolocation to apply the policy based on the user's location. *Id.*

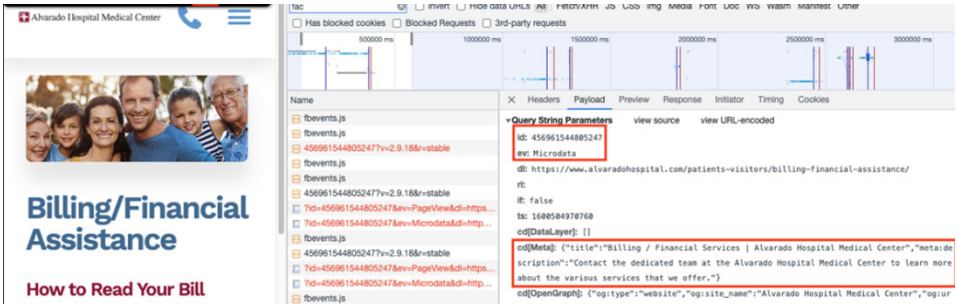




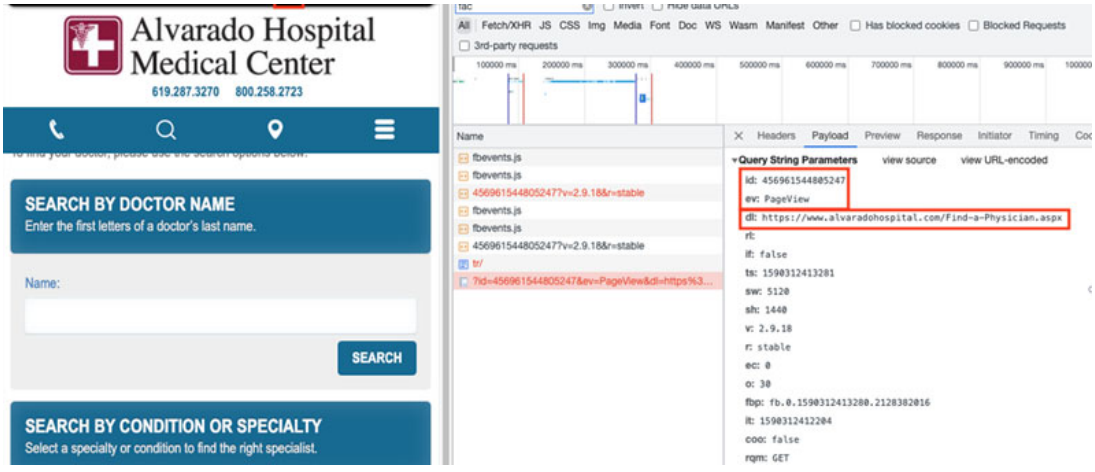
87. As Users moved beyond the homepage, Prime Healthcare continued to disclose user details through PageView, Microdata, and SubscribedButtonClick events. Prime Healthcare disclosed users': (i) appointment booking activities; (ii) browsing medical conditions and treatments; (iii) bill payment activities; (iv) accessing the patient portal; (v) submission of forms containing personal medical information; and (vi) the text of users' searches for medical treatment information.

88. For example, Prime Healthcare also shared details about Users' bill payment activities. When a User navigated to the Online Bill Payment page, Prime Healthcare would send PageView and Microdata events revealing that the user was on the page for "Billing/Financial Assistance." Both events inform Facebook that the User was on the page "patients-visitors" looking for "billing-financial assistance." *See* Figures 5-6:

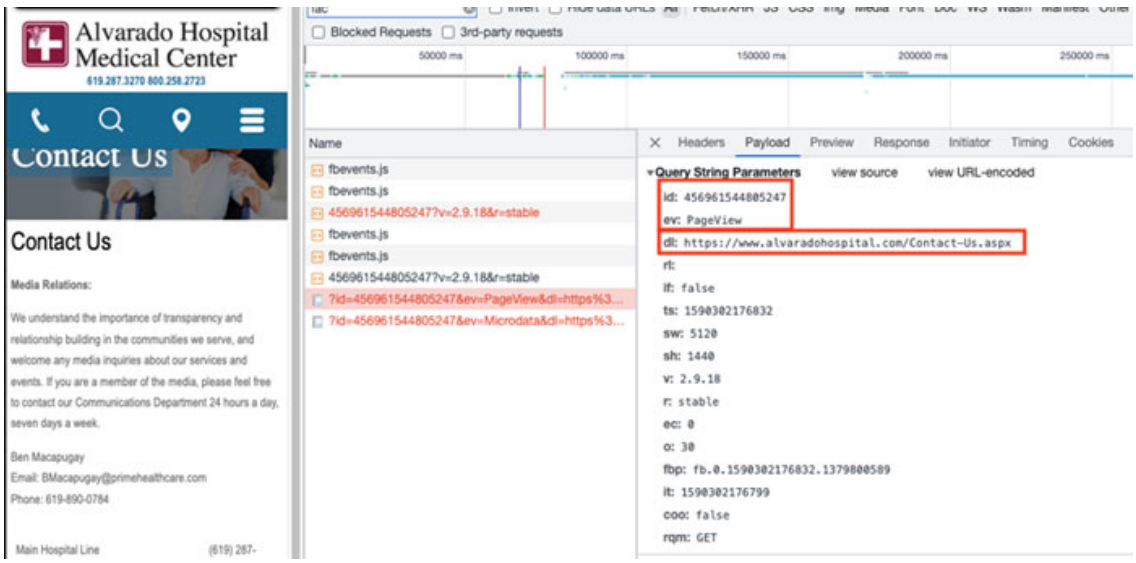




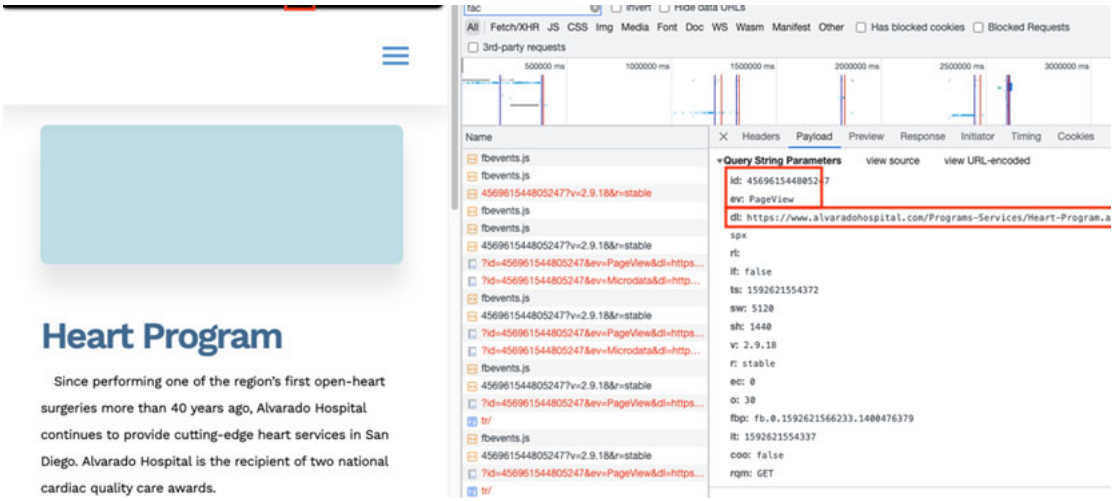
89. When a User searched for a doctor, Prime Healthcare would also send that information to Facebook through PageView and Microdata events, *See* Figure 7:



90. Prime Healthcare would also have disclosed when users tried to contact Prime Healthcare. As a user landed on the "Contact Us" page, Prime Healthcare would disclose that by sending PageView and Microdata events. The Microdata event informs Facebook that the user was attempting to contact Alvarado Hospital, *See* Figure 8:

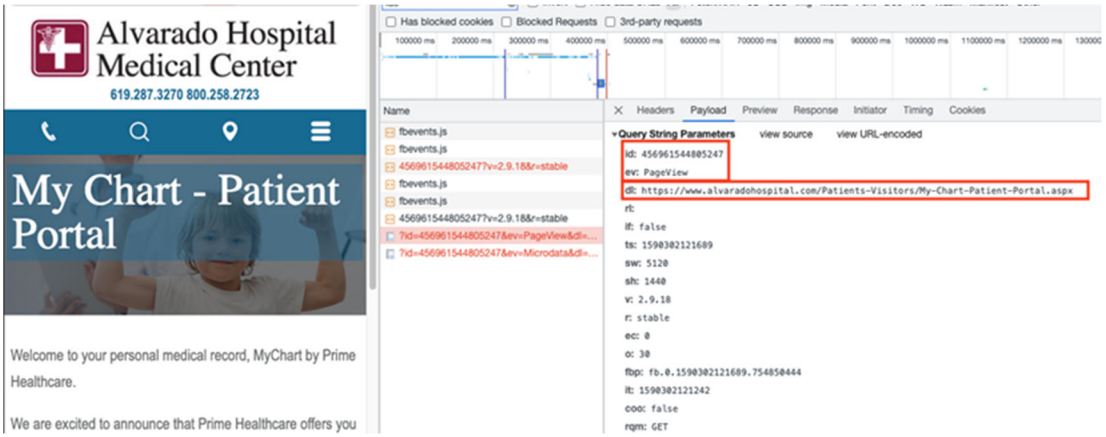


91. In addition to users' search for doctors and seeking to contact Defendant, Prime Healthcare also shared information about services users explored.

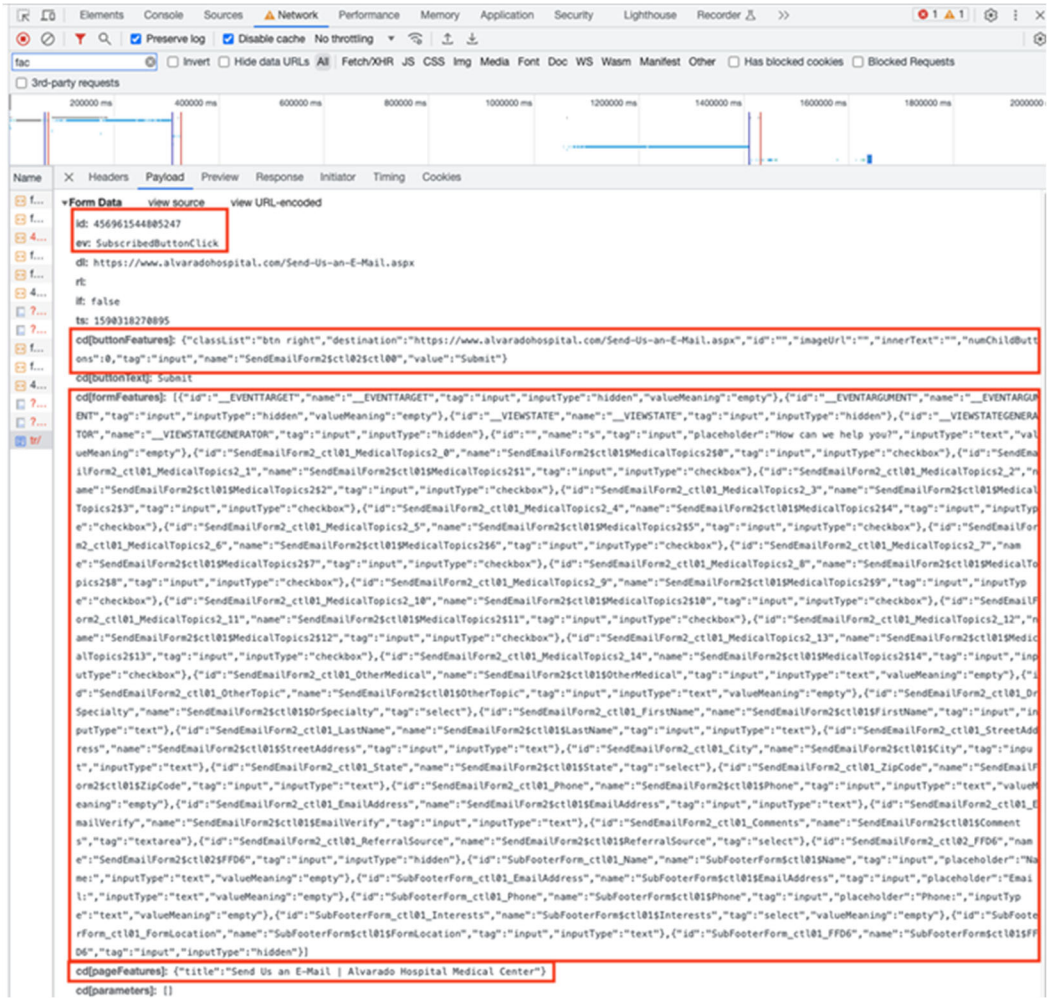


92. For example, when a user navigated to view Prime Healthcare's cardiology services, Prime Healthcare would send PageView and Microdata events to Facebook revealing that the user searching for Defendant's "Heart Program" Program" *See* Figure 9:

93. Prime Healthcare also informed Facebook when Users viewed pages about Prime Healthcare's patient Portal. Upon a User loading the page to access Prime Healthcare's patient Portal, Prime Healthcare would send PageView and Microdata events. The Microdata event informs Facebook that the User was on the page for "Patients-Visitors/My-Chart-Patient-Portal." *See* Figure 10:

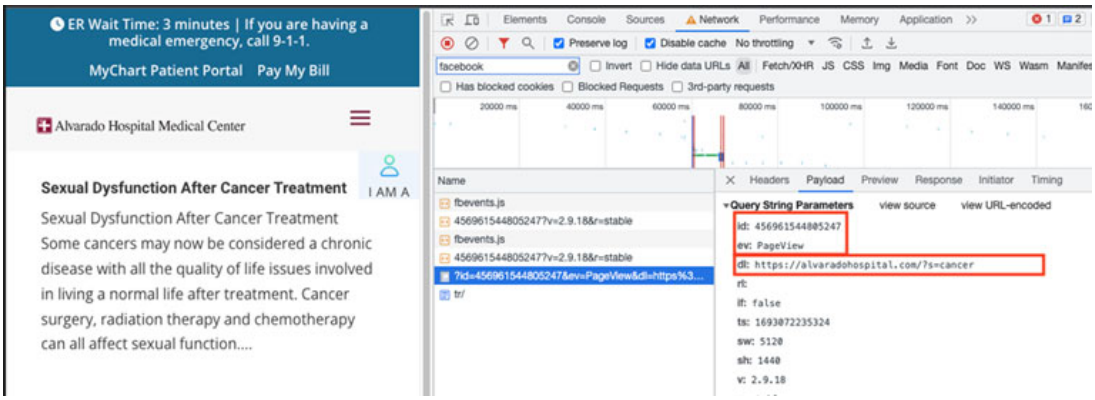


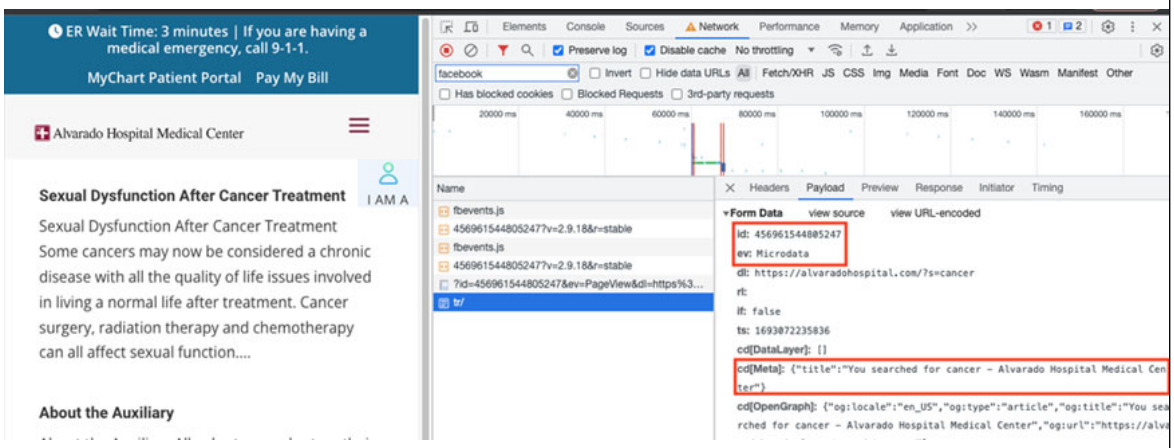
94. Prime Healthcare also disclosed when users submitted forms where the Users entered data. For example, Prime Healthcare provides a form for Users to email their healthcare provider. When a User filled out the form and clicked submit, Prime Healthcare would send a SubscribedButtonClick event to Facebook, disclosing that the user sent their provider an email. *See* Figure 11:



95. Finally, when Users searched Prime Healthcare's Web Properties for information concerning their medical conditions and treatments for those conditions, Prime Healthcare disclosed the specific text

of those search queries. For example, when a User typed "cancer" into Prime Healthcare's search bar, Prime Healthcare would disclose the contents of that search by including the Users' search queries in the "dl" parameter in PageView and Microdata events and in the cd[Meta] parameter in the Mircrodata event. In this case, Prime Healthcare would disclose to Facebook "s-cancer" in PageView and "You searched for cancer" in Microdata. *See* Figures 12-13:





E. Facebook's Platform & its Business Tools.

96. Facebook operates the world's largest social media company and generated $117 billion in revenue in 2021.[36] Roughly 97% of that came from selling advertising space.[37]

97. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Prime Healthcare, to utilize its "Business Tools" to gather, identify, target, and market products and services to individuals.

98. Facebook's Business Tools, including the Meta Pixel, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

99. In particular, the Meta Pixel "tracks the people and type of actions they take."[38]

100. The User's web browser (software applications that allow consumers to exchange electronic communications over the Internet) executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner.

---

[36] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Feb. 6, 2024).

[37] *Id.*

[38] *Retargeting*, *supra* note 7.

101. The Pixel is thus customizable and programmable, meaning that the website owner controls which of its web pages contain the Pixel and which events are tracked and transmitted to Facebook.

102. The process of adding the Pixel to webpages is a multi-step process that must be undertaken *by the website owner*.[39]

103. Facebook guides the website owner through setting up the Pixel during the setup process. Specifically, Facebook explains that there are two steps to set up a pixel:

> 1. Create your pixel and set up the pixel base code on your website. You can use a partner integration if one is available to you or you can manually add code to your website.
>
> 2. Set up events on your website to measure the actions you care about, like making a purchase. You can use a partner integration, the point-and-click event setup tool, or you can manually add code to your website.[40]

104. Aside from the various steps to embed and activate the Pixel, website owners, like Prime Healthcare, must also agree to Facebook's Business Tools Terms by which Facebook requires website owners using the Meta Pixel to "represent and warrant" that they have adequately and prominently notified users about the collection, sharing and usage of data through Facebook's Business Tools (including the Pixel and Conversions

---

[39] *Business Help Center: How to set up and install a Meta Pixel*, https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited Feb. 6, 2024); *see* Ivan Mana, *How to Set Up & Install the Facebook Pixel (in 2022)*, https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited Feb. 6, 2024).

[40] *Id*.

API)[41] and that websites "will not share Business Tool Data . . . that [websites] know or reasonably should know . . . includes health, financial information or other categories of sensitive information . . . ."[42]

105. Once fully loaded and operational, the Pixel prompts the Users' web browser to transmit specific information based on parameters set by the website owner. This customizable nature of the Meta Pixel allows the website owner to determine which webpages contain the Pixel, which events are tracked and shared with Facebook and whether the tracked events are standard (chosen from the list of 18 provided by Facebook) or custom (defined by the website owner). For example, the Pixel can be set to capture the URLs visited by website visitors via a "PageView" event, or to capture the exact inner text of buttons clicked by a visitor, via a "SubscribedButtonClick" event.

106. The Business Tools are automatically configured to capture "Standard Events," such as when a user visits a particular webpage, that

---

[41] *Meta Business Tools Terms*, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfbOvnb7E0sZ-wzgCW6xNLFKEOEVH_fr6JjkMINTJNqN7i1R-3MPh5caFgmdgAOxbL8&_rdr (last visited Feb. 6, 2024) ("When you use any of the Meta Business Tools to send us or otherwise enable the collection of Business Tool Data . . ., these Business Tools Terms govern the use of that data").

[42] *Id.*; *see also* Pratyush Deep Kotoky, *Facebook collects personal data on abortion seekers: Report* (June 16, 2022) https://www.newsbytesapp.com/news/science/facebook-collects-personal-data-on-abortion-seekers/story (quoting Facebook spokesman Dale Hogan as saying that it is "against [Facebook's] policies for websites and apps to send sensitive health data about people through [its] Business Tools") (last visited Feb. 6, 2024).

webpage's Universal Resource Locator ("URL") and metadata, button clicks, etc.[43]

107. Advertisers, such as Prime Healthcare, can track other User actions and can create their own tracking parameters by building a "custom event."[44]

108. When a user accesses a webpage that is hosting the Meta Pixel, their communications and interactions with the host webpage are instantaneously and surreptitiously sent to Facebook's servers—traveling from the user's browser to Facebook's server.[45]

109. This simultaneous secret transmission contains the original GET request sent to the host website, along with additional data that the Meta Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and

---

[43] *Specifications for Facebook Pixel Standard Events*, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Feb. 6, 2024); *see also* META PIXEL, GUIDES, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/ (last visited Feb. 6, 2024); BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142 (last visited Feb. 6, 2024); APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Feb. 6, 2024).

[44] ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Feb. 6, 2024).

[45] Plaintiff unequivocally and in good faith pleads that Prime Healthcare's Pixel transmissions to Facebook occur simultaneously as Users navigate and use Prime Healthcare's Web Properties.

read Prime Healthcare's Websites—Prime Healthcare's own code and Facebook's embedded code.

110. Prime Healthcare tracked Users and disclosed Users' events including at least the following:

- Users' search queries;
- When Users clicked to use the patient portal;
- When Users clicked to access and view the bill page;
- When Users clicked to request an appointment; and
- What care and treatment options Users viewed.

111. Accordingly, during the same transmissions, the Websites routinely provide Facebook with Prime Healthcare patients' Facebook IDs, IP addresses and/or device IDs, and the other information they input into Prime Healthcare's Websites, including their medical searches, treatment requests, and the webpages they view.

112. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[46] Plaintiff's and Class Members' identities can be easily determined based on the Facebook ID, IP address, and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

113. Instead of taking proactive steps to verify that businesses using the Pixel obtain the required consent, Meta uses an "honor system" under which Meta assumes these businesses have "provided robust and sufficient prominent notice to users regarding the Business Tool Data collection, sharing, and usage."[47]

---

[46] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Feb. 6, 2024).

[47] *See* Facebook Business Tools Terms,

114. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. When the Website visitor is also a Facebook user, the information collected via the Meta Pixel is associated with the User's Facebook ID that identifies their name and Facebook profile—their real-world identity.

115. The Pixel collects data regardless of whether the visitor has an account. Facebook maintains "shadow profiles" on Users without Facebook accounts and links the information collected via the Meta Pixel to the User's real-world identity using their shadow profile.[48]

116. A User's Facebook ID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access and view the User's corresponding Facebook profile. To find the Facebook account associated with a c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

117. The Private Information disclosed via the Pixel allows Facebook to know that a specific patient is seeking confidential medical care and the type of medical care being sought. Facebook then uses that information to

---

https://www.facebook.com/legal/terms/businesstools.

[48] *See* Russell Brandom, *Shadow Profiles Are the Biggest Flaw In Facebook's Privacy Defense*, (Apr 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Feb. 6, 2024).

sell advertising to Prime Healthcare and other advertisers and/or sells that information to marketers who use it to online target Plaintiff and Class Members.

118. Facebook (as well as other unauthorized third-party recipients of information captured by these invisible tracking codes) tracks user data and communications for its own marketing purposes and for the marketing purposes of the website owner. Ultimately, the purpose of collecting user data is to make money.

119. Thus, without any knowledge, authorization or action by a user, website owners like Prime Healthcare use source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

120. In this case, Prime Healthcare employed the Pixel, among other tracking technologies, to intercept Plaintiff's and Class Members' Private Information to Facebook (and the other tracking code information recipients such as Google).

121. In sum, the Pixel and other tracking technologies on the Website permitted Facebook and any other Pixel information recipient to intercept the content of Plaintiff's and Class Members' highly sensitive communications and Private Information , which communications contained private and confidential medical information.

122. These interceptions of Plaintiff's and Class Members' communications content were performed without Plaintiff's or Class Members' knowledge, consent, or express written authorization.

F. Meta Encourages Healthcare Partners, Including Prime Healthcare, to Upload Patient Lists for Ad Targeting.

123. Meta operates the world's largest social media company. Meta's revenue is derived almost entirely from selling targeted advertising. Meta's Health division is dedicated to marketing to and servicing Meta's healthcare partners. Meta defines its Partners to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

124. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

125. Meta offers an ad targeting option called "Custom Audiences."

126. When a patient takes an action on a Meta healthcare partner's website embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta matches to its users.

127. A web developer can then create a "Custom Audience" based on Events to target ads to those patients.

128. The Pixel can then be used to measure the effectiveness of an advertising campaign.[49]

---

[49] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9d

129. Meta also allows Meta healthcare partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[50]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

130. Meta provides detailed instructions for healthcare partners to send their patients' Private Information to Meta through the customer list upload. For example:[51]

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

---

ff7fa.

[50] Meta Business Help Center, *About Customer List Custom Audiences* (2023), https://www.facebook.com/business/help/341425252616329?id=2469097953376494.

[51] *Create a customer list custom audience*,

131. Meta healthcare partners can then use the Custom Audiences derived from their patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

G. Prime Healthcare's Use of the Pixels Violated Its Own Privacy Policies.

132. Defendant publishes several privacy policies that represent to patients and visitors to its Web Properties that it will keep Private Information private and secure and that it will only disclose PII and PHI provided to it under certain circumstances, ***none of which apply here***.

133. Defendant's Privacy Policy acknowledges that Prime Healthcare is required by law to make sure that medical information that identifies patients is kept private and describes some of the legally permitted ways for Defendant to use and to disclose patients' medical information.[52]

134. Patients and other visitors to the Website are not informed about, and have not consented to, the collection of their Personal Health Information ***and*** Website activity or to providing that information to a third party.

135. Prime Healthcare's Privacy Policy states:

> **Information Collection, Use, and Sharing**
>
> We are the sole owners of the information collected on this site. We only have access to/collect information that you voluntarily give us via email or other direct contact from you. We will not sell or rent this information to anyone.

---

https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Feb. 6, 2024).

[52] https://www.primehealthcare.com/policies/ (last visited Jan. 23, 2024).

> We will use your information to respond to you, regarding the reason you contacted us. We will not share your information with any third party outside of our organization, other than as necessary to fulfill your request, e.g. to ship an order.
> …
>
> **Cookies**
>
> We use "cookies" on this site. A cookie is a piece of data stored on a site visitor's hard drive to help us improve your access to our site and identify repeat visitors to our site. For instance, when we use a cookie to identify you, you would not have to log in a password more than once, thereby saving time while on our site. Cookies can also enable us to track and target the interests of our users to enhance the experience on our site. Usage of a cookie is in no way linked to any personally identifiable information on our site.
>
> Some of our business partners may use cookies on our site (for example, advertisers). However, we have no access to or control over these cookies.
>
> **Sharing**
>
> We share aggregated demographic information with our partners and advertisers. This is not linked to any personal information that can identify any individual person.[53]

136. Prime Healthcare's promises that its use of cookies "is in no way linked to any personally identifiable information", that Prime Healthcare "will not share your information with any third party outside of our organization, other than as necessary to fulfill your request, e.g. to ship an order," and that Prime Healthcare Prime Healthcare has no access to or control over the cookies its business partners place on its Websites, are false.[54]

137. The Pixel, which is embedded in and throughout the Websites, collects search queries regarding medical conditions, treatment, and/or specific providers. Even non-Facebook users can be individually identified

[53] *Id.*

[54] *Id.*

via the information gathered on the Websites like an IP address or personal device identifying information.

138. This is precisely the type of information for which HIPAA requires healthcare providers to utilize de-identification techniques to protect the privacy of patients.[55]

139. Despite a lack of disclosure, Defendant allows Facebook to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information that it promises to keep private.

140. Prime Healthcare breached its own privacy policies by unlawfully permitting Facebook and likely other third parties to intercept Users' Private Information without obtaining patients' consent or authorization. Facebook then read, understood, and used that Private Information for its own business purposes—i.e., selling targeted advertising to Prime Healthcare and others which specifically targeted those Users based on their health conditions.

H. Prime Healthcare Violated HIPAA.

141. Defendant's disclosure of Plaintiff's and Class Members' Private Information to entities like Facebook also violated HIPAA.

142. Under federal law, a healthcare provider may not disclose PII, non-public medical information about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[56]

[55] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Jan. 15, 2024).

[56] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

143. Guidance from HHS instructs healthcare providers that patient status alone is protected by HIPAA.

144. HIPAA's Privacy Rule defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and either (i) "identifies the individual;" or (ii) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

145. The Privacy Rule broadly defines protected health information as individually identifiable health information that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

146. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (i) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination'" or (ii) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

A. Names;
…
H. Medical record numbers;
…
J. Account numbers;
…

> M. Device identifiers and serial numbers;
> N. Web Universal Resource Locators (URLs);
> O. Internet Protocol (IP) address numbers; … and
> P. Any other unique identifying number, characteristic, or code… and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information."[57]

147. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of PHI without authorization. 45 C.F.R. §§ 160.103, 164.502.

148. Even the fact that an individual is receiving a medical service, *i.e.*, is a patient of a particular entity, can be PHI.

149. HHS has instructed health care providers that, while identifying information alone is not necessarily PHI if it were part of a public source such as a phonebook because it is not related to health data, "[i]f such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI."[58]

150. Consistent with this restriction, HHS has issued marketing guidance that provides, "With limited exceptions, the [Privacy] Rule requires an individual's written authorization before a use or disclosure of his or her

---

[57] *See* 45 C.F.R. § 160.514.

[58] *See Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Feb. 6, 2024).

protected health information can be made for marketing . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list."[59]

151. Here, as described *supra*, Prime Healthcare provided patient information to third parties in violation of the Privacy Rule—and its own Privacy Policy. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."

152. The statute states that a "person … shall be considered to have obtained or disclosed individually identifiable health information … if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

153. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually identifiable health information relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both." 42 U.S.C. § 1320(d)(6)(b)(1).

[59] *Marketing*, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html (last visited Feb. 6, 2024).

154. HIPAA also requires Prime Healthcare to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights," 45 C.F.R. § 164.312(a)(1)—which Prime Healthcare failed to do.

155. Under HIPAA, Prime Healthcare may not disclose PII about a patient, potential patient or household member of a patient for marketing purposes without the patient's express written authorization. *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

156. Prime Healthcare further failed to comply with other HIPAA safeguard regulations as follows:

a) Failing to ensure the confidentiality and integrity of electronic PHI that Prime Healthcare created, received, maintained and transmitted in violation of 45 C.F.R. section 164.306(a)(1);

b) Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

c) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Prime Healthcare in violation of 45 C.F.R. section 164.308(a)(6)(ii);

d) Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. section 164.306(a)(2);

e) Failing to protect against reasonably anticipated uses or disclosures of electronic PHI not permitted under the privacy rules pertaining to

individually identifiable health information in violation of 45 C.F.R. section 164.306(a)(3); and

f) Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

157. In disclosing the content of Plaintiff's and Class Members' communications, Prime Healthcare had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions, that is, to illegally disclose Plaintiff's and Class Members' Private Information to Facebook (and other unauthorized third party data brokers) in violation of HIPAA, including 42 U.S.C. § 1320d-6(a)(3), as well as the torts alleged below. Defendant would not have been able to obtain the Private Information or the marketing services it did if it had complied with the law.

158. Commenting on a June 2022 report discussing the use of Meta Pixels by hospitals and medical centers, David Holtzman, a health privacy consultant and a former senior privacy adviser in HHS OCR, which enforces HIPAA, stated, "I am deeply troubled by what [the hospitals] are doing with the capture of their data and the sharing of it … It is quite likely a HIPAA violation."[60]

159. Prime Healthcare's placing third-party tracking codes on its Web Properties is a violation of Plaintiff's and Class Members' privacy rights under federal law. While Plaintiff does not bring a claim under HIPAA

[60] ADVISORY BOARD, '*Deeply Troubled*': *Security experts worry about Facebook trackers on hospital sites*, https://www.advisory.com/daily-briefing/2022/06/17/data-trackers (last visited Feb. 6, 2024).

itself, this violation demonstrates Prime Healthcare's wrongdoing relevant to other claims and establishes its duty to maintain patient privacy.

I. Prime Healthcare's Use of the Pixel Violates OCR Guidance.

160. The government has issued guidance warning that tracking technologies like the Pixel may come up against federal privacy law when installed on healthcare websites.

161. Healthcare organizations regulated under the HIPAA may use third-party tracking tools, such as Pixels or Google Analytics *only in a limited way* to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors.[61]

162. According to the Bulletin, Prime Healthcare has violated HIPAA rules by implementing the Pixel.[62]

163. Prime Healthcare has shared Plaintiff's and Class Members' Private Information, including health conditions for which they seek treatments, treatments and/or medications sought, the frequency with whom they take steps to obtain healthcare for certain conditions, and their unique identifiers. This information is, as described in the OCR Bulletin, "highly sensitive."

164. The OCR Bulletin goes on to make clear how broad the government's view of protected information is as it explains:

> This information might include an individual's medical record number, home or email address, or

[61] *See* OCR Bulletin, *supra,* note 12.

[62] *See id*. ("disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures").

> dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code***.[63]

165. Prime Healthcare's sharing of Private Information with the Pixel Information Recipients violated Plaintiff's and Class Members' rights.

J. Prime Healthcare Violated Industry Standards.

166. A medical provider's duty of confidentiality is embedded in the physician-patient and hospital-patient relationship—it is a cardinal rule.

167. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

168. AMA Code of Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)[.] [64]

169. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient

[63] *Id.* (emphasis added).

[64] https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/code-of-medical-ethics-chapter-3.pdf (last visited Feb. 6, 2024).

> whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.[65]

170. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must: (c) Release patient information only in keeping with ethics guidelines for confidentiality.[66]

171. Prime Healthcare's use of the Pixels also violates FTC data security guidelines. The FTC has promulgated numerous guides for businesses, which highlight the importance of implementing reasonable data security practices.

172. The FTC's October 2016 publication *Protecting Personal Information: A Guide for Business*[67] established cyber-security guidelines for businesses. These guidelines state that businesses should protect the personal patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network vulnerabilities, and implement policies to correct any security problems.

173. In fact, the FTC has recently brought enforcement actions against several healthcare companies, including Premom, BetterHelp,

---

[65] *Id*.

[66] *Id*.

[67] *See* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 6, 2024).

GoodRx, and Flow Health for conveying information—or enabling an inference—about their consumers' health to unauthorized third parties without the consumers' consent.

174. Like the health care companies fined by the FTC in recent years, Prime Healthcare failed to implement these basic, industry-wide data security practices.

K. Users' Reasonable Expectation of Privacy.

175. Plaintiff and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

176. Indeed, when Plaintiff and Class Members provided their PII/PHI to Defendant, they each had a reasonable expectation that the information would remain private, and that Defendant would not share the Private Information with third parties for a commercial purpose unrelated to patient care.

177. Privacy polls and studies show that the overwhelming majority of Americans consider obtaining an individual's affirmative consent before a company collects and shares its customers' data to be one of the most important privacy rights.

178. For example, a recent Consumer Reports study shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumer data, and the same percentage believe those companies and websites should be required to provide consumers with a complete list of the data that is collected about them.[68]

[68] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-

179. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

180. Plaintiff's and Class Members' reasonable expectations of privacy in their PII/PHI are grounded in, among other things, Defendant's status as a healthcare provider, Defendant's common law obligation to maintain the confidentiality of patients' PII/PHI, state and federal laws protecting the confidentiality of medical information, state and federal laws protecting the confidentiality of communications and computer data, state laws prohibiting the unauthorized use and disclosure of personal means of identification, and Defendant's express and implied promises of confidentiality.

L. Unique Personal Identifiers are Protected Health Information.

181. While not all health data is covered under HIPAA, the law specifically applies to healthcare providers, health insurance providers, and healthcare data clearinghouses.[69]

182. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information that is held or transmitted, and there are approximately 18 HIPAA Identifiers that are considered PII. This

---

confident-about-healthcare-data-privacy-and-car-safety-a3980496907/ (last visited Feb. 6, 2024).

[69] *See* Alfred Ng & Simon Fondrie-Teitler, *This Children's Hospital Network Was Giving Kids' Information to Facebook* (June 21, 2022), https://themarkup.org/pixel-hunt/2022/06/21/this-childrens-hospital-network-was-giving-kids-information-to-facebook (stating that "[w]hen you are going to a covered entity's website, and you're entering information related to scheduling an appointment, including your actual name, and potentially other identifying characteristics related to your medical condition, there's a strong possibility that HIPAA is going to apply in those situations") (last visited Feb. 6, 2024).

information can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

183. These HIPAA Identifiers, as relevant here, include, device identifiers, web URLs and IP addresses.[70]

184. Prime Healthcare improperly disclosed Plaintiff's and Class Members' HIPAA identifiers, including their computer IP addresses, device identifiers, and web URLs visited to the Pixel Information Recipients through their use of the Pixel *in addition to* services selected, patient statuses, medical conditions, treatments, provider information, and appointment information.

185. An IP address is a number that identifies the address of a device connected to the Internet. IP addresses are used to identify and route communications on the Internet. IP addresses of individual Internet users are used by Internet service providers, websites, and third-party tracking companies to facilitate and track Internet communications.

186. Facebook tracks every IP address ever associated with a Facebook user (and with non-users through shadow profiles). Google also tracks IP addresses associated with Internet users.

187. Facebook, Google, and other third-party marketing companies track IP addresses to target individual homes and their occupants with advertising.

188. Under HIPAA, an IP address is considered personally identifiable information, which is defined as including "any unique

---

[70] *Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Feb. 6, 2024).

identifying number, characteristic or code," specifically listing IP addresses among examples. *See* 45 C.F.R. § 164.514 (2).

189. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

190. Consequently, Prime Healthcare's disclosure of Plaintiff's and Class Members' IP addresses violated HIPAA and industry-wide privacy standards.

M. Prime Healthcare was Enriched by & Benefitted from the Use of the Pixel & Other Tracking Technologies.

191. One of the primary reasons that Prime Healthcare decided to embed the Pixel and other tracking technologies on its Web Properties with the purpose of disclosing Plaintiff's and Class Members's communications to Facebook and other third party data brokers in order to improve marketing by creating campaigns that maximize conversions and thereby decrease costs to Prime Healthcare and boost its revenue.

192. After receiving individually identifiable patient health information communicated on Prime Healthcare's Web Properties, Facebook analyzes this data, improves its own technology and business (including machine learning), and then forwards this data and analysis of this data, to Prime Healthcare.

193. Prime Healthcare then uses this data and analysis for its own commercial purposes that include understanding how Users utilize its Web Properties.

194. Facebook, as well, uses this data and analysis for its own commercial purposes, including to improve its platform and better understand the individuals that make up the audiences that its clients (advertisers) pay Facebook to target with ads.

195. Prime Healthcare also receives an additional commercial benefit from using Facebook's tracking tools, such as the Meta Pixel, in being able to serve more targeted advertisements to existing and prospective patients on their Meta accounts such as Facebook and Instagram.

196. Facebook advertises its Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting."[71]

197. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. In particular, retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[72]

198. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Prime Healthcare's Web Properties. For example, when a User

[71] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited Feb. 6, 2024).

[72] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Feb. 6, 2024).

searches for doctors or medical conditions or treatment on Prime Healthcare's Web Properties, that information is sent to Facebook. Facebook can then use its data on the User to find more users to click on a Prime Healthcare ad and ensure that the targeted Users are more likely to convert.[73]

199. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures "includes URL names of pages visited, and actions taken—all of which could be potential examples of health information."[74]

200. Plaintiff's and Class Members' Private Information has considerable value as highly monetizable data, especially insofar as it allows companies to gain insight into their customers so that they can perform targeted advertising and boost their revenues.

201. In exchange for disclosing the Private Information of their account holders and patients, Prime Healthcare is compensated by the Private Information recipients, such as Facebook, in the form of enhanced advertising services and more cost-efficient marketing on their platform.

202. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because

[73] *See, e.g.*, *How to Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking* (Mar. 14, 2023), https://www.freshpaint.io/blog/how-to-make-facebook-ads-hipaa-compliant-and-still-get-conversion-tracking (last visited Feb. 6, 2024).

[74] *Id*.

many such trackers are not HIPAA-compliant or are only HIPAA-compliant if certain steps are taken.[75]

203. For example, Freshpaint, a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant. They don't sign BAAs, and the Meta Pixel acts like a giant personal user data vacuum sending PHI to Meta servers," and "[i]f you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[76]

204. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[77]

205. Whether a user has a Facebook profile is not indicative of damages because Facebook creates shadow profiles, and at least one court has recognized that the pixels' ability to track comprehensive browsing history is also relevant. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1078–79 (N.D. Cal. 2021) (finding a reasonable expectation of privacy where Google combined the unique identifier of the user it collects from websites and Google Cookies that it collects across the internet on the same user).

---

[75] *See The guide to HIPAA compliance in analytics,* https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Feb. 6, 2024).

[76] *How To Make Facebook Ads HIPAA Compliant and Still Get Conversion Tracking*, *supra* note 73.

[77] *The complex world of healthcare retargeting, supra* note 72.

206. Upon information and good faith belief, Prime Healthcare retargeted patients and potential patients, including Plaintiff and Class Members.

207. Thus, utilizing the Pixels directly benefits Prime Healthcare by, among other things, reducing the cost of advertising and retargeting.

N. Plaintiff's Private Information is Extremely Valuable.

208. Plaintiff's and Class Members' Private Information has value, and Prime Healthcare's disclosure and interception harmed Plaintiff and the Class by not compensating them for the value of their Private Information and, in turn, decreasing the value of their Private Information.

209. Tech companies are under particular scrutiny because they already have access to a massive trove of information about people, which they use to serve their own purposes, including potentially micro-targeting advertisements to people with certain health conditions.

210. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

211. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[78] A 2015 article from TechCrunch accurately noted that "[d]ata has become a strategic asset that allows companies to acquire or maintain a competitive edge."[79] That article noted that the value of

[78] *See* https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Feb. 6, 2024).

[79] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Feb. 6, 2024).

a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

212. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data (after costs).[80] That figure is only due to keep increasing; estimates for 2022 were as high as $434 per user, for a total of more than $200 billion industry wide.

213. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[81]

214. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[82]

---

[80] *See What Your Data is Really Worth to Facebook* (July 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/ (last visited Feb. 6, 2024).

[81] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

[82] *See 10 Apps for Selling Your Data for Cash*, https://wallethacks.com/apps-for-selling-your-data/ (last visited Feb. 6, 2024).

215. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

216. Courts recognize the value of personal information and the harm when it is disclosed without consent. *See, e.g., In re Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014) (holding that plaintiffs' allegations that they were harmed by the dissemination of their personal information and by losing the sales value of that information were sufficient to show damages for their breach of contract and fraud claims); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (recognizing "the value that personal identifying information has in our increasingly digital economy").

217. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

218. Healthcare data is incredibly valuable because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been sold. Once it has been detected, it can take years to undo the damage caused.

219. The value of health data is well-known and various reports have been conducted to identify its value.

220. Specifically, in 2023, the Value Examiner published a report entitled Valuing Healthcare Data. The report focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of

"such data should ensure it is priced at fair market value to mitigate any regulatory risk."[83]

221. Trustwave Global Security published a report entitled The Value of Data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[84]

222. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[85]

223. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[86]

224. The dramatic difference in the price of healthcare data compared to other forms of private information commonly sold is evidence of the value of PHI.

---

[83] *See* https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Feb. 6, 2024).

[84] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (last visited Feb. 6, 2024) (citing https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf).

[85] *See* https://time.com/4588104/medical-data-industry/ (last visited Feb. 6, 2024).

[86] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Feb. 6, 2024).

225. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

226. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

227. Prime Healthcare shared Plaintiff's and Class Members' communications and transactions on its Web Properties without permission.

228. The unauthorized access to Plaintiff's and Class Members' personal and Private Information has diminished the value of that information, resulting in harm to Web Properties Users, including Plaintiff and Class Members.

229. Plaintiff has a continuing interest in ensuring that her future communications with Prime Healthcare are protected and safeguarded from future unauthorized disclosure.

REPRESENTATIVE PLAINTIFF R.S.'S EXPERIENCES

230. Plaintiff R.S. accessed and used the Web Properties using computers and/or devices located in California to seek medical treatment and/or advice as recently as 2022.

231. R.S. has been a patient of Prime Healthcare at Centinella Hospital since approximately 2012. She has been treated for a variety of medical conditions including for blood work, back and leg pain, bunions and foot pain, and certain gynecological conditions.

232. R.S. began using the Centinella website and Patient Portal in approximately 2018. R.S. used these Web Properties to find doctors, make appointments and research medical treatments and conditions.

233. The information that R.S. provided to Defendant's Web Properties and Portal included queries about her medical conditions including for bunions and foot pain and menopause, as well as searches for podiatrists and gynecologists, including by name.

234. R.S. has had a Facebook account for more than 10 years.

235. After she was seen at Prime and looked for information about menopause on Defendant's Web Properties, R.S. began receiving ads for menopause medication on Facebook.

236. Plaintiff R.S. reasonably expected that her communications with Prime Healthcare via the Web Properties were confidential, solely between herself and Prime Healthcare, and that such communications would ***not*** be transmitted to or intercepted by any third party without her full knowledge and informed consent.

237. Plaintiff R.S. provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

238. As described herein, Defendant worked along with Facebook to intercept Plaintiff R.S.'s communications, including those that contained Private and confidential information, while Plaintiff R.S. was within the state of California.

239. Defendant willfully facilitated these interceptions without Plaintiff R.S.'s knowledge, consent, or express written authorization.

240. Within the State of California, Defendant transmitted Plaintiff R.S.'s FID, computer IP address, location, and information such as her medical conditions including menopause, treatment sought, appointment type, physician selected including gynecologist and podiatrist, and button/menu selections to Facebook.

241. By doing so without her consent, Defendant breached Plaintiff R.S.'s right to privacy and unlawfully disclosed her Private Information.

242. Defendant did not inform Plaintiff R.S. that it shared her Private Information with Facebook.

243. Plaintiff R.S. suffered damages in, *inter alia*, the form of (i) invasion of privacy; (ii) violation of confidentiality of her Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to her Private Information.

244. Plaintiff R.S. has a continuing interest in ensuring that her Private Information is protected and safeguarded from future unauthorized disclosure. Plaintiff R.S. wants to continue to communicate with Defendant's healthcare providers through online platforms but has no practical way of knowing if her communications are being intercepted and disclosed to Facebook, and thus continues to be at risk of harm from Prime Healthcare's conduct.

TOLLING

245. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiff did not know (and had no way of knowing) that her Private Information was intercepted and unlawfully disclosed because Defendant kept this information secret. Plaintiff only discovered that her Private Information had been disclosed by Defendant in September 2023.

CLASS ACTION ALLEGATIONS

246. Class Definition**:** Pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and other similarly situated individuals (the "Class"), as

defined below.

247. The **Nationwide Class** that Plaintiff seeks to represent is defined as:

> All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the third-party tracking technologies on Defendant Prime Healthcare's Websites and/or Web Properties.

248. Plaintiff reserves the right to modify the class definition or add sub-classes as necessary prior to filing a motion for class certification.

249. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after consideration of any tolling, concealment, and accrual issues, and ending on the date of entry of judgment.

250. Excluded from the Class is Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

251. Numerosity/Ascertainability. Members of the Class are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class Members is unknown to Plaintiff at this time. However, it is estimated that there are at least thousands of individuals in the Class. The identity of such membership is readily ascertainable from Defendant's records and non-party Facebook's records.

252. Typicality. Plaintiff's claims are typical of the claims of the Class because Plaintiff used the Website and had their personally identifiable information and protected health information disclosed to Facebook without

their express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class Members.

253. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the Class Members. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the Class.

254. Common Questions of Law and Fact Predominate/Well-Defined Community of Interest. Questions of law and fact common to the Class predominate over questions that may affect only individual Class Members because Defendant has acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent in Defendant's wrongful conduct. The following questions of law and fact are common to the Class:

a. Whether and to what extent Defendant had a duty to protect the Plaintiff's and Class Members' Private Information;

b. Whether Defendant had duties not to disclose Plaintiff's and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant violated its privacy policy by disclosing Plaintiff's and Class Members' Private Information to Facebook, Meta, or other third parties;

d. Whether Defendant adequately, promptly and accurately informed Plaintiff and Class Members that their Private Information would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient Private Information;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Defendant knowingly made false representations as to its data security and/or privacy policy practices;

j. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy policy practices;

k. Whether Defendant's acts and practices violated Plaintiff's and Class Members' privacy rights;

l. Whether Plaintiff and Class Members are entitled to actual, consequential or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Defendant knowingly made false representations as to it data security and/or privacy policy practices;

n. Whether Defendant knowingly omitted material representations with respect to its data security and/or privacy

policy practices;

o. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their Private Information;

p. Whether Plaintiff and Class Members are entitled to damages under CIPA, the CMIA, or any other relevant statute; and

q. Whether Defendant's actions violate Plaintiff's and Class Members' privacy rights as provided by the California Constitution.

255. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff is unaware of any special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

CLAIMS FOR RELIEF

COUNT I

VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq.*
Unauthorized Interception, Use & Disclosure
(On behalf of Plaintiff & the Nationwide Class)

256. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the proposed Class.

223. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

224. The ECPA protects both sending and receipt of communications.

225. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

226. The transmissions of Plaintiff's PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

227. Electronic Communications. The transmission of PII and PHI between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

228. Content. The ECPA defines content, when used with respect to electronic communications, to "include[] ***any information concerning the substance, purport, or meaning of that communication***." 18 U.S.C. § 2510(8) (emphasis added).

229. Interception. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents

. . . include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

230. Electronical, Mechanical, or Other Device. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5).

231. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Defendant and Meta use to track Plaintiff's and the Class Members' communications;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing devices;

d. Defendant's web-servers; and

e. The Pixels deployed by Defendant to effectuate sending and acquiring Users' and patients' sensitive communications.

232. Plaintiff and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

233. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

234. Specifically, Defendant intercepted Plaintiff's and Class Members' electronic communications via the Meta Pixel, Conversions API and other tracking technologies, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such as Facebook.

235. Defendant intercepted communications that include, but are not

limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, including IP address, Facebook ID, treatment information, medications and scheduling details. Additionally, through the above-described tracking tools, Defendant transmitted the communications about doctors, treatments and conditions, including but not limited to the name(s), location(s) and specialty(s) of physicians' Plaintiff searched for on Defendant's Web Properties. This information was, in turn, used by third parties, such as Facebook, to 1) place Plaintiff in specific health-related categories and 2) target Plaintiff with particular advertising associated with Plaintiff's specific health conditions.

236. Defendant knowingly transmits this data and does so for the purpose of financial gain.

237. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

238. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

239. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States—namely, invasion of privacy, among others.

240. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply.

The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information (IIHI) to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual*, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[87]

241. Plaintiff's information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6).

242. Defendant used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

243. Defendant was not acting under color of law to intercept

[87] *Id.* § 1320d-(6) (emphasis added).

Plaintiff's and the Class Members' wire or electronic communication.

244. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's privacy via the Pixel tracking code. Plaintiff and absent class members (all of whom are patients) had a reasonable expectation that Defendant would not re-direct their communications content to Facebook, Google or other third parties attached to their personal identifiers in the absence of their knowledge or consent.

245. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

246. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendant's Web Properties, researching medical conditions and treatment and scheduling appointments with doctors, Defendant's purpose was tortious, criminal and designed to violate federal and state legal provisions including a knowing intrusion into a private place or matter that would be highly offensive to a reasonable person.

247. Consumers have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that cause Facebook pixels and cookies (including but not limited to the fbp, fr, and datr cookies) and other tracking technologies to be deposited on Plaintiff's and Class members' computing devices as "first-party" cookies that are not blocked.

248. Defendant's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the claims below;

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Meta.

249. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property:

a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

250. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiff's and Class Members' property:

a. with knowledge that (1) Defendant did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their Private Information based on their activities on Defendant's Website; (4) "a reasonable Facebook user would be shocked to realize" the extent of Meta's collection of Private Information; (5) a Covered Incident had occurred which required a

report to be made to the FTC pursuant to Meta's consent decrees with the FTC and (6) the subsequent use of health information for advertising was a further invasion of such property rights in making their own exclusive use of their Private Information for any purpose not related to the provision of their healthcare; and

b. with the intent to (1) acquire Plaintiff and Class Members' Private Information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use Plaintiff's and Class Members' Private Information without their authorization and (3) gain access to Plaintiff's and Class Members' personal computing devices through the 'fbp' cookie disguised as a first-party cookie.

251. A person who violates § 2511(1)(a) is liable for $10,000 in statutory damages to any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used.

252. As a direct and proximate result of Defendant's violation of the ECPA, Plaintiff and Class Members were damaged by Defendant's conduct.

253. For the reasons set forth, Defendant is liable to Plaintiff and Class Members for violations of the ECPA.

254. Based on the foregoing, Plaintiff and Nationwide Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

RELIEF REQUESTED

257. Plaintiff, individually and on behalf of the proposed Class, respectfully requests that the Court grant the following relief:

a. Certification of this action as a class action and appointment of Plaintiff and Plaintiff's counsel to represent the Class;

b. An order enjoining Defendant from engaging in the unlawful practices and illegal acts described herein; and

c. An order awarding Plaintiff and the Class: (1) actual or statutory damages; (2) punitive damages – as warranted – in an amount to be determined at trial; (3) prejudgment interest on all amounts awarded; (4) injunctive relief as the Court may deem proper; (5) reasonable attorney fees and expenses and costs of suit pursuant to the ECPA, California Code of Civil Procedure § 1021.5 and/or other applicable law; and (6) Such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the proposed Class, demands a trial by jury for all claims asserted herein and so triable.

DATED: February 8, 2024

/s/ Daniel Srourian

Daniel Srourian
California Bar No. 285678
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd. Suite 1710
Los Angeles, CA 90010
daniel@slfla.com

John R. Parker, Jr.
California Bar No. 257761
ALMEIDA LAW GROUP LLC
jrparker@almeidalawgroup.com
3550 Watt Avenue, Suite 140
Sacramento, California 95608
Tel: (916) 616-2936

David S. Almeida (*pro hac vice forthcoming*)
Matthew J. Langley
California Bar No. 342846
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
t: 312-576-3024
david@almeidalawgroup.com
matt@almeidalawgroup.com

Attorneys for Plaintiff & the Class